

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN**

Brandi McKenzie, *on behalf of herself and all
others similarly situated,*

Plaintiff,

v.

Henry Ford Health System,

Defendant.

COMPLAINT - CLASS ACTION

JURY TRIAL DEMANDED

Case No. 23-CV-11796

CLASS ACTION COMPLAINT

Plaintiff, Brandi McKenzie (“Plaintiff”), brings this Class Action Complaint (“Complaint”) against Defendant, Henry Ford Health System (“Defendant”), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, and upon information and belief and her counsels’ investigation as to all other matters, as follows:

INTRODUCTION

1. Plaintiff seeks monetary damages and injunctive and declaratory relief arising from Defendant’s failure to safeguard the Personally Identifiable Information¹ (“PII”) and Protected Health Information (“PHI”) (together, “Private Information”) of its patients, which resulted in unauthorized access to its information systems on or around March 30, 2023 and the compromised

¹ The Federal Trade Commission (“FTC”) defines “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the subject data breach.

and unauthorized disclosure of that Private Information, causing widespread injury and damages to Plaintiff and the proposed Class (defined below) members.

2. Defendant, one of the largest health systems in Michigan “is one of the nation’s leading academic medical centers,” and “is consistently ranked among the top NIH institutions in Michigan.”² Defendant “provides a full continuum of services – from primary and preventative care, to complex and specialty care, health insurance, a full suite of home health offerings, virtual care, pharmacy, eye care and other healthcare retail.”³ Defendant “serves a growing number of customers across 250+ locations throughout Michigan including five acute care hospitals, two destination facilities for complex cancer and orthopedic and sports medicine care, three behavioral health facilities, primary care and urgent care centers.”⁴

3. As explained in detail herein, on or around March 30, 2023, Defendant’s systems were subject to a cyberattack via an email phishing scheme, whereby an unauthorized individual or individuals were able to access Defendant’s business email accounts. Defendant reports that patient information was exposed in the compromised mailboxes and confirmed internally on May 16, 2023 that “protected health information was contained” in the compromised email boxes (the “Data Breach”).⁵

4. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of Defendant’s patients, including Plaintiff and the proposed Class members, were stolen, including their names, genders, dates of birth, ages, lab results, procedure types, diagnoses, dates of service, telephone numbers, medical record numbers and/or internal tracking numbers.⁶

² <https://www.henryford.com/about> (last accessed July 24, 2023).

³ *Id.*

⁴ *Id.*

⁵ See Notice Letter to Plaintiff, attached as **Exhibit A**.

⁶ *Id.*

5. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and approximately 168,000 other individuals' information (together, "Patients").⁷

6. Despite being aware of the Data Breach since at least May 16, 2023, Defendant did not post a notification on its website announcing the Data Breach until on or around July 14, 2023 and began sending notifications to impacted individuals on or around July 14, 2023.⁸

7. Defendant's failure to safeguard Patients' highly sensitive Private Information as exposed and unauthorizedly disclosed in the Data Breach violates its common law duty, Michigan law, and Defendant's implied contract with its Patients to safeguard their Private Information.

8. Plaintiff and Class members now face a lifetime risk of identity theft due to the nature of the information lost.

9. Defendant's harmful conduct has injured Plaintiff and Class members in multiple ways, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

10. Defendant's failure to protect Patients' Private Information has harmed and will continue to harm over tens of thousands of Defendants' Patients, causing Plaintiff to seek relief on a class wide basis.

11. On behalf of herself and the Classes preliminarily defined below, Plaintiff brings

⁷ <https://www.wfla.com/news/hillsborough-county/1-2-million-affected-by-tampa-general-hospital-data-breach/> (last accessed July 24, 2023).

⁸ See Exhibit A.

causes of action against Defendant for negligence, negligence *per se*, breach of implied contract, and violation of the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.901 *et seq.*, seeking an award of monetary damages and injunctive and declaratory relief, resulting from Defendant's failure to adequately protect their highly sensitive Private Information.

PARTIES

12. Plaintiff is, and at all times mentioned herein was, an individual resident and citizen of the State of Michigan.

13. Plaintiff provided Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information.

14. If Plaintiff had known that Defendant would not adequately protect her Private Information, she would not have allowed Defendant to maintain this sensitive Private Information.

15. Defendant is a corporation organized under the laws of Michigan with its principal place of business in Detroit, Michigan.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District. Defendant has sufficient contacts in Michigan, as it conducts a significant amount of its business in the state of Michigan.

18. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL BACKGROUND

Defendant's Business

19. Defendant employs 33,000 people, and "serves a growing number of customers across 250+ locations throughout Michigan including five acute care hospitals, two destination facilities for complex cancer and orthopedics and sports medicine care, three behavioral health facilities, primary care and urgent care centers."⁹ Due to the nature of these the services it provides, Defendant acquires and electronically stores Patients' Private Information. As a healthcare provider, Defendant is required to ensure that Private Information is not disclosed or disseminated to unauthorized third parties without its Patients' express written consent.

20. Plaintiff and Class members are current or former Patients who provided their Private Information to Defendant.

21. To obtain medical services, Patients, including Plaintiff and Class members, were required to provide sensitive and confidential Private Information, including their names, genders, dates of birth, ages, telephone numbers, and other sensitive information, that would be held by Defendant in its computer systems.

22. The information held by Defendant at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class members.

23. Upon information and belief, Defendant made promises and representations to its Patients that the Private Information collected would be kept safe and confidential, the privacy of

⁹ About Henry Ford Health, available at <https://www.henryford.com/about> (last visited July 24, 2023).

that information would be maintained, and Defendant would delete any sensitive information after it was no longer required to maintain it.

24. Indeed, Defendant's own Notice of Privacy Practices acknowledges that it is "required by HIPAA to make sure that medical information that identifies you is kept private . . . and to follow the terms of the Notice that is currently in effect."¹⁰

25. The Notice of Privacy Practices further provides that "[a]s permitted by HIPAA and Michigan State law, we may use or disclose your medical information without obtaining prior authorization from you to carry out the activities detailed below." Those "activities" do not encompass the Data Breach."¹¹

26. Defendant's "Privacy Fact Sheet" identifies "Types of security threats faced today by health care providers," which include "[h]acker and disgruntled employee abuse."¹²

27. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

¹⁰ Notice of privacy practices, <https://www.henryford.com/visitors/privacy/practices> (last visited July 24, 2023).

¹¹ *Id.*

¹² Privacy Fact Sheet, <https://www.henryford.com/visitors/privacy/fact-sheet> (last visited July 24, 2023).

29. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep Patients' Private Information safe and confidential.

30. Defendant had obligations under the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

31. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

The Data Breach

33. On or about July 14, 2023, Defendant began notifying Patients of the Data Breach, informing them:

Henry Ford Health is notifying some of their patients that an unauthorized individual conducted an email phishing scheme to gain access to business email accounts. The improper access was quickly discovered and the email accounts were secured.

Here are important facts to know:

- Some of patient information was contained in the affected email boxes, but we don't know whether such information was actually accessed or not.
- Phishing email schemes are used to fraudulently obtain victims' credentials or personal information by sending them fake email messages.

The incident occurred on March 30, 2023 and we immediately began an extensive investigation to determine what happened. Through our forensics investigation, we

determined on May 16, 2023 that protected health information was contained in the email boxes and could have been accessed by the bad actor.

The information stored on the affected email accounts may have included the following: name, gender, date of birth, age, lab results, procedure type, diagnosis, date of service, telephone number, medical record number and/or internal tracking number.

As a result of this incident, we are implementing additional security measures and providing additional training to employees about recognizing the signs of suspicious email and what to do if they receive one.

If there are questions, please call our Incident Response Line at **833-627-2685 between 9 a.m. and 9 p.m. Eastern Time, Monday - Friday**. That number goes to our business partner, Epiq Solutions, a call center based in Portland, Oregon that specializes in providing assistance for data security and cybersecurity incidents and services for other industries.¹³

34. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

35. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class members, including their names, genders, dates of birth, ages, lab results, procedure types, diagnoses, dates of service, telephone numbers, medical record numbers and/or internal tracking numbers. Plaintiff's and Class members' Private Information was accessed and stolen in the Data Breach.

36. Plaintiff further believes her Private Information, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

¹³ https://www.henryford.com/-/media/files/hfh-patient-data-breach-substitute-notice-final-71423_pdf.pdf?rev=c4c7bc44f5b34de991947c5fe870d6d7&hash=1DCEC46FDA0242BF2BB609F790397C28 (last visited July 24, 2023).

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information.

37. As a condition to obtain medical services from Defendant, Plaintiff and Class members were required to give their sensitive and confidential Private Information to Defendant.

38. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class members' Private Information, Defendant would be unable to perform its services.

39. By obtaining, collecting, and storing the Private Information of Plaintiff and Class members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

40. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

41. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class members.

42. Upon information and belief, Defendant made promises to Plaintiff and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

43. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Entities in Possession of Private Information Are Particularly Susceptable to Cyber Attacks.

44. Data thieves regularly target entities in the healthcare industry like Defendant due to the highly sensitive information that they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

45. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities like Defendant that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

46. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

47. Indeed, in December 2017, Defendant disclosed a data breach involving the PHI of nearly 20,000 patients after "[s]omeone gained access to or stole the e-mail credentials of a group of employees."¹⁴

48. Of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7%, were in the medical or healthcare industry.¹⁵

¹⁴ Nearly 20,000 patients compromised by Henry Ford Health System data breach, Detroit Free Press, Dec. 6, 2017, <https://www.freep.com/story/news/local/michigan/detroit/2017/12/06/henry-fordhospital-data-breach/926163001/> (last visited July 24, 2023).

¹⁵ 2021 Data Breach Annual Report (ITRC, Jan. 2022), <https://notified.idtheftcenter.org/s/>, at 6.

49. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.¹⁶

50. Entities in custody of PHI and/or medical information reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.¹⁷ Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the “average total cost to resolve an identity theft-related incident . . . came to about \$20,000,” and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.¹⁸ Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.¹⁹

51. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from being compromised.

52. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s server(s), amounting to over one million individuals’

¹⁶ *Id.*

¹⁷ See Identity Theft Resource Center, *2022 Annual Data Breach Report*, <https://www.idtheftcenter.org/publication/2022-data-breach-report/> (last accessed May 8, 2023).

¹⁸ See Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July 24, 2023).

¹⁹ See *id.*

detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

53. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

54. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

55. As a healthcare entity in possession of its Patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Fails to Comply with FTC Guidelines

56. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

57. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.²⁰

58. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²¹

59. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's

²⁰ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed July 24, 2023).

²¹ *Id.*

data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

62. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

63. Defendant failed to properly implement basic data security practices.

64. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to Patients’ Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

65. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its Patients; Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant’s conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails to Comply with HIPAA Guidelines.

66. Defendant is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health

Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

67. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).²² See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

68. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

69. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

70. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

71. “Electronic protected health information” is “individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

72. HIPAA’s Security Rule requires Defendant to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

²² HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

d. Ensure compliance by its workforce.

73. HIPAA also requires Defendant to “review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

74. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. § 17902.

75. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

76. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

77. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed

guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.²³ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.²⁴

Defendant Owed Plaintiff and Class Members a Duty to Safeguard their Private Information.

78. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class members.

79. Defendant owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

²³ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

²⁴ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last accessed July 24, 2023).

80. Defendant owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

81. Defendant owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

82. Defendant owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

83. Defendant owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiff's and Class Members' Risk of Identity Theft.

84. The unencrypted Private Information of Plaintiff and Class members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

85. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members.

86. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class members because of the Data Breach.

87. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

88. Plaintiff's and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used

in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

89. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

90. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class members must monitor their financial and personal accounts for many years to mitigate the risk of identity theft.

91. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

92. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."²⁵

93. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach,

²⁵ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf> (last accessed July 24, 2023).

including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁶

94. And for those Class members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”

Diminution of Value of Private Information.

95. Private Information is valuable property.²⁷ Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

96. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably name—is difficult, if not impossible, to change.

97. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit

²⁶ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last accessed July 24, 2023).

²⁷ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” at 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last accessed July 24, 2023) (“GAO Report”).

card information, personally identifiable information . . . [is] worth more than 10x on the black market.”²⁸

98. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.²⁹

99. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.³⁰ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{31,32} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50 a year.³³

100. As a result of the Data Breach, Plaintiff’s and Class members’ Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an

²⁸ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed July 24, 2023).

²⁹ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

³⁰ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last accessed July 24, 2023).

³¹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last accessed July 24, 2023).

³² <https://datacoup.com/> (last accessed July 24, 2023).

³³ <https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer> (last accessed July 24, 2023).

economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

101. The fraudulent activity resulting from the Data Breach may not come to light for years.

102. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

103. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

104. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.

105. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

106. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

107. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

108. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear, but for Defendant's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

109. Furthermore, Defendant's poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing to pay Defendant for the provision of its services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

110. Plaintiff obtained medical services from Defendant. To obtain these medical services, she was required to provide her Private Information to Defendant.

111. Upon information and belief, at the time of the Data Breach—March 30, 2023—Defendant retained Plaintiff’s Private Information in its system.

112. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

113. Plaintiff received notice of the Data Breach on or about July 14, 2023.³⁴ According to the Defendant, some of Plaintiff’s information was contained in the employee email boxes affected in the Data Breach, and the information stored on the affected email account may have included Plaintiff’s name, gender, date of birth, age, lab results, procedure type, diagnosis, date of service, telephone number, medical record number and/or internal tracking number.³⁵

114. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including checking her bills and accounts to make sure they were correct. Plaintiff has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

115. As a result of the Data Breach, Plaintiff fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

³⁴ See Exhibit A.

³⁵ *Id.*

116. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

117. As a result of the Data Breach, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

118. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

119. Pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff brings this action on behalf of herself and on behalf of all members of the proposed Nationwide Class and Michigan Subclass (together, the "Class" or "Classes") defined as:

Nationwide Class: All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported to have occurred on or about March 30, 2023.

Michigan Subclass: All individuals residing in the state of Michigan whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported to have occurred on or about March 30, 2023.

120. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

121. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

122. **Numerosity:** The Class members are so numerous that joinder of all members is impracticable, if not completely impossible. Approximately 168,000 individuals were affected by the of the Data Breach. The Class is apparently identifiable within Defendant's records, as Defendant has sent notice of the Data Breach to Plaintiff and other Class members.

123. Common questions of law and fact exist as to all Class members and predominate over any questions affecting solely individual Class members. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, are the following:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class members;
- b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the Private Information of Plaintiff and Class members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class members;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

- g. Whether Plaintiff and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and
- h. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

124. **Typicality:** Plaintiff's claims are typical of those of the other Class members because Plaintiff, like every other Class member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

125. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

126. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of Class members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiff seeks no relief that is antagonistic or adverse to Class members and the infringement of the rights and the damages she has suffered are typical of other Class members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

127. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that millions of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

128. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

129. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

130. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

- a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- b. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to breach of an implied contract;
- e. Whether Defendant's failure to institute adequate protective security measures violated FDUTPA;
- f. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- g. Whether adherence to HIPAA and FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

131. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in paragraphs 1 through 130.

132. Defendant requires its Patients, including Plaintiff and Class members, to submit non-public Private Information in the ordinary course of providing health plan services.

133. Defendant gathered and stored the Private Information of Plaintiff and Class members as part of its business of soliciting its services to its Patients, which solicitations and services affect commerce.

134. Plaintiff and Class members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

135. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

136. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

137. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

138. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

139. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its Patients. That special relationship arose because Plaintiff and Class members entrusted Defendant with their confidential Private Information, a necessary part of being Patients of Defendant.

140. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

141. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

142. Defendant breached its duties, thus was negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class members' Private Information.

143. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly considering Defendant's inadequate security practices.

144. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

145. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

146. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and Class members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

147. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

148. Plaintiff and Class members had no ability to protect their Private Information that was in, and likely remains in, Defendant's possession.

149. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

150. Defendant's duty extended to protecting Plaintiff and Class members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

151. Defendant has admitted that the Private Information of Plaintiff and Class members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

152. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, the Private Information of Plaintiff and Class members would not have been compromised.

153. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class members and the harm, or risk of imminent harm, suffered by Plaintiff and Class members. The Private Information of Plaintiff and Class members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

154. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

155. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

156. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

157. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

158. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Nationwide Class)

159. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in paragraphs 1 through 130.

160. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

161. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq.*, Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information.

162. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

163. Defendant breached its duties to Plaintiff and Class members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

164. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

165. The injuries to Plaintiff and Class members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

166. Plaintiff and Class members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

167. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

168. The injuries and harms suffered by Plaintiff and Class members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiff and

Class members to experience the foreseeable harms associated with the exposure of their Private Information.

169. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

170. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 130.

171. Defendant offered to provide services to its Patients, including Plaintiff and Class members, in exchange for payment.

172. Defendant also required Plaintiff and the Class members to provide Defendant with their Private Information to receive services.

173. In turn, Defendant impliedly promised to protect Plaintiff's and Class members' Private Information through adequate data security measures.

174. Plaintiff and the Class members accepted Defendant's offer by providing Private Information to Defendant in exchange for receiving Defendant's services, and then by paying for and receiving the same.

175. Plaintiff and Class members would not have entrusted their Private Information to Defendant but for the above-described agreement with Defendant.

176. Defendant materially breached its agreement(s) with Plaintiff and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

177. Plaintiff and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

178. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

179. Defendant’s conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

180. The losses and damages Plaintiff and Class members sustained as described herein were the direct and proximate result of Defendant’s breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

COUNT IV
Violation of the Michigan Consumer Protection Act,
Mich. Compl. Laws Ann. § 445.901 *et seq.*
(On behalf of Plaintiff and the Michigan Subclass)

181. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 130.

182. Plaintiff and the Michigan Subclass are “persons” as defined by Mich. Comp. Laws Ann. § 445.903(d).

183. Defendant advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

184. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);
- b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);
- c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and
- d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

185. Defendant's unfair, unconscionable, and deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect the Private Information of Plaintiff and the Michigan Subclass, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiff and the Michigan

Subclass, including duties imposed by HIPAA and the FTC Act, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of the Private Information of Plaintiff and the Michigan Subclass, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiff and the Michigan Subclass, including duties imposed by HIPAA and the FTC Act;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure the Private Information of Plaintiff and the Michigan Subclass; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiff and the Michigan Subclass, including duties imposed by HIPAA and the FTC Act.

186. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of Patients' Private Information.

187. Defendant intended to mislead Plaintiff and the Michigan Subclass and induce them to rely on its misrepresentations and omissions.

188. Defendant acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded the rights of Plaintiff and the Michigan Subclass.

189. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff and the Michigan Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

190. Plaintiff and the Michigan Subclass seek all monetary and nonmonetary relief allowed by law, including the greater of actual damages or \$250, restitution, injunctive relief, and any other relief that is just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class members, requests judgment against Defendant and that the Court grants the following:

- A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class members;

- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:
- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.
 - iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;
 - iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class members;
 - v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class members on a cloud-based database;
 - vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and security checks;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis to evaluate Defendant's

compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined by a jury at trial;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: July 25, 2023.

Respectfully submitted,

By: Jeff Ostrow
Jeff Ostrow
Kristen Lake Cardoso
Steven Sukert
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
ostrow@kolawyers.com
cardoso@kolawyers.com
sukert@kolawyers.com

*Attorneys for Plaintiff and the Putative
Classes*